S&H Form: (02/05)

REPLY/AMENDMENT FEE TRANSMITTAL

Attorney Docket No.	1341.1076
Application Number	09/739,645
Filing Date	December 20, 2000
First Named Inventor	Masahiro KOMURA et al.
Group Art Unit	2136
Examiner Name	Carl G. Colin

AMOUNT ENCLOSED	500.00

FEE CALCULATION (fees effective 12/08/04)

CLAIMS AS AMENDED	Claims Remaining After Amendment	Highest Number Previously Paid For	Number Extra	Rate	Calculations
TOTAL CLAIMS	16	- 20 =	0	X $ 50.00 =	$ 0.00
INDEPENDENT CLAIMS	4	- 4 =	0	X $ 200.00 =	0.00

Since an Official Action set an original due date of _, petition is hereby made for an extension to cover the date this reply is filed for which the requisite fee is enclosed (1 month ($120)); (2 months ($450)); (3 months ($1,020)); (4 months ($1,590)); (5 months ($2,160):	
If Appeal Brief is enclosed, add ($500.00)	500.00
If Statutory Disclaimer under Rule 20(d) is enclosed, add fee ($130.00)	
Information Disclosure Statement (Rule 1.17(p)) ($180.00)	
Total of above Calculations =	$ 500.00
Reduction by 50% for filing by small entity (37 CFR 1.9, 1.27 & 1.28)	
TOTAL FEES DUE =	$ 500.00

(1) If entry (1) is less than entry (2), entry (3) is "0".

(2) If entry (2) is less than 20, change entry (2) to "20".

(4) If entry (4) is less than entry (5), entry (6) is "0".

(5) If entry (5) is less than 3, change entry (5) to "3".

METHOD OF PAYMENT

☒ Check enclosed as payment.

☐ Charge "TOTAL FEES DUE" to the Deposit Account No. below.

☐ No payment is enclosed.

GENERAL AUTHORIZATION

☒ If the above-noted "AMOUNT ENCLOSED" is not correct, the Commissioner is hereby authorized to credit any overpayment or charge any additional fees necessary to:

Deposit Account No.	19-3935
Deposit Account Name	STAAS & HALSEY LLP

☒ The Commissioner is also authorized to credit any overpayments or charge any additional fees required under 37 CFR 1.16 (filing fees) or 37 CFR 1.17 (processing fees) during the prosecution of this application, including any related application(s) claiming benefit hereof pursuant to 35 USC § 120 (e.g., continuations/divisionals/CIPs under 37 CFR 1.53(b) and/or continuations/divisionals/CPAs under 37 CFR 1.53(d)) to maintain pendency hereof or of any such related application.

SUBMITTED BY: STAAS & HALSEY LLP

Typed Name	Luminita A. Todor	Reg. No.	57,639
Signature	L Todor	Date	Sept. 15, 2006

Docket No.: 1341.1076

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Masahiro KOMURA et al.

Serial No. 09/739,645 Group Art Unit: 2136

Confirmation No. 4243

Filed: December 20, 2000 Examiner: Carl G. Colin

For: METHOD AND APPARATUS FOR MEDIATION OF SECURITY INFORMATION, AND A COMPUTER PRODUCT

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief-Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In a Notice of Appeal filed July 20, 2006, Applicants appealed the Examiner's March 27, 2006 Office Action finally rejecting claims 1-17. Submitted herewith are an Appeal Brief, and the requisite fees set forth in 37 C.F.R.§ 41.20(b).

I. REAL PARTY IN INTEREST

The real party in interest is Fujitsu Limited, the assignee of this application.

II. RELATED APPEALS AND INTERFERENCES

Appellant, appellant's legal representative, and the assignee do not know of any prior or pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by, or have a bearing on, the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1-17 have been rejected and are on appeal.

IV. STATUS OF AMENDMENTS

No amendment has been filed following the Final Office Action rejecting claims 1-17, which was mailed on March 27, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A. Claim 1

Independent claim 1 is directed to a security information mediation apparatus. The security information mediation apparatus, for example, 20 in FIG. 1 or 200 of FIG. 4 or 600 of FIG. 8 or 1000 of FIG. 12, is connected between a first terminal, for example, user client 11 of FIG. 1 or any of 101A and 101B of FIG. 4 or 501 of FIG. 8 or any of 501 and 901 of FIG 12, at an information contributor, for example, the user 10 of FIG. 1 or any of 100A and 100B of FIG.4 or 500 of FIG. 8 or any of 500 and 900 of FIG. 12 and a second terminal, for example, any of the developer clients 30 A and 30 B of FIG. 1 or 300 of FIG. 4 or any of 700A and 700B of FIG. 8 and FIG 12 at an information recipient, for example, any of the developers 31A and 31B of FIG. 1, 301 of FIG. 4, any of 301A and 301B of FIG. 8 and 12. Page 9, line 21 through page 10 line 5, page 17 line 25 through page 20 line 7, page 30 line 1through page 31 line 12, page 42 lines 12-21.

Claim 1 recites that the security information mediation apparatus comprises a first receiving unit, for example, the receiving unit 201 in FIG. 4 or 601 in FIGS. 8 and 12, which receives security information from the first terminal. See page 21 lines 5-13, page 32 lines 4-6 and page 43 lines 13-16. The security information includes information regarding a design error or bug in a computer program as illustrated in FIGS. 2A, 5A-B and 9A and described in page 10 lines 15-21, page 18 lines 20-23, page 30 lines 23-25. A first registering unit, for example, 21 in FIG. 1, registers the security information in a first database, for example 22 in FIG. 1, which feature is described on page 12, lines 13-21. A first transfer unit, for example 23 in FIG. 1, receives the security information from the first registering unit and transfers the security information registered by the first registering unit to the second terminal for the information recipient to judge usefulness of the security information, as described on page 12 lines 22-25.

According to claim 1, a second receiving unit, for example, 206 in FIG.4 or 607 in FIGS. 8 and 12, receives at least reply information including the usefulness of the security information corresponding to the security information from the second terminal, as described, for example, on page 22, lines 13-18, page 35 lines 5-9, and page 43 lines 4-9. A second registering unit, for example, 24 in FIG. 1, registers at least the reply information in a second database, for example, 25 if FIG.1, as described on page 13 line 24 through page 14 line 4. A second transfer unit, for example, 26 in FIG 1, 207 in FIG.4 and 608 in FIGS. 8 and 12, receives at least the reply information from the second registering unit and transfers the reply information to the first terminal, as described on page 14 lines 4-11, page 23 lines 21-24, and page 36 lines 10-13.

Claim 1 also recites that when the information recipient finds that the security information has usefulness, the second receiving unit receives payment information on an information presentation fee to be paid to the information contributor from the second terminal, the second registering unit registers the payment information together with the reply information, and the second transfer unit transfers the payment information together with the reply information to the first terminal. See page 15 line 9 through page 17 line 10 and FIG. 1 items 41A, 41B and 42.

B. Claims 8 and 15

Independent claim 8 is directed to a security information mediation method.

Claim 8 recites the security information mediation method including receiving security information from a first terminal (e.g., 11 in FIG. 1) at an information contributor (e.g. 10 in FIG. 1), the security information comprising information regarding a design error or bug in a computer program. This operation is illustrated, for example in SA1 of FIG. 3 or SB1 of FIG. 7 which is described on page 24 lines 11-13.

Claim 8 further recites first registering the security information in a first database (e.g., 22, in FIG. 1), for example, operation SA2 in FIG. 3 described on page 14 line 23-25. Claim 8 also recites receiving the security information registered at the first registering and transferring the security information registered at the first registering to a second terminal (e.g. 30 A or B of FIG. 1) at an information recipient (e.g., 31 A or B of FIG. 1) for judging usefulness of the security information, for example, see SA3 of FIG. 3 described on page 15 lines 1-5.

Additionally, claim 8 recites receiving at least reply information including the usefulness of the security information corresponding to the security information from the second terminal, for example, SA4 of FIG. 3 which is described on page 15 line 25 through page 16 line1.

Claim 8 further recites registering at least the reply information in a second database (e.g., 25 of FIG. 1), for example, SA7 or SA9 of FIG. 3 described on page 15 lines 10-12 and on page 9 lines 15-17, respectively.

Claim 8 also recites receiving at least the reply information and transferring the reply information to the first terminal, for example, SA8 of FIG. 3 which is described on page 16 lines 12-17.

Claim 8 also specifies that when the information recipient (e.g., 31 A or B of FIG. 1) finds that the security information has usefulness, the receiving of at least the reply information includes receiving payment information on an information presentation fee to be paid to the information contributor (e.g., 10 in FIG. 1) from the second terminal (e.g. 30 A or B of FIG. 1), the registering of at least the reply information includes registering the payment information together

with the reply information (e.g., SA7 of FIG. 3), and the receiving at least the reply information and transferring includes transferring the payment information together with the reply information to the first terminal (e.g., SA8 of FIG. 3).

Claim 15 is directed to "a computer readable medium for storing instructions which when executed by a computer causes the computer to execute" substantially the method of claim 8. FIG. 17 and page 54, lines 1-25 provide support to the preamble of claim 15.

C. Claim 16

Claim 16 is directed to a method of collecting information over a network comprising determining that the information (e.g., 40 in FIGS. 1 and 2A) regarding a design error or bug in a computer program, which information is received from a verified user (e.g., SB1-SB3 in FIG. 7) is valuable (see, for example, page 25, lines 15-17). According to claim 16, the method further includes rewarding the user for submitting the information (e.g., SB6-SB10 in FIG. 7 and page 26, lines 2-23).

D. Claim 17

Claim 17 is directed to a method of collecting information over a network comprising determining that the information (e.g., 400A and B in FIG. 4) regarding a design error or bug in a computer program (e.g. FIG. 5 A or B), which information is received from a verified user (e.g., SB1-SB3 in FIG. 7) is valuable (see, for example, page 25, lines 15-17). According to claim 16, the method further includes rewarding the user for submitting the information (e.g., SB6-SB10 in FIG. 7 and page 26, lines 2-23).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The only ground of rejection to be reviewed is the rejection of claims 1-17 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,327,578 to Linehan ("Linehan") in view of U.S. Patent No. 5,761308 to Torii et al. ("Torii").

VII. ARGUMENT

A. Review of the Prior Art

1. U.S. Patent No. 6,327,578 to Linehan

Linehan is directed to a method, system and program for electronic commerce using a four party payment protocol for electronic sales including a consumer's computer coupled to a merchant's computer and to an issuing bank computer via an issuer gateway. The merchant computer is further coupled to an acquiring bank computer (see Claim 1, FIG. 2A of Linehan). Linehan discloses an arrangement which allows moving the credit/debit card authorization function from the merchant to the issuer so that an issuer can independently choose alternate authentication mechanisms without changing the acquirer gateway.

2. U.S. Patent No. 5,761,308 to Torii et al.

Torii is directed to a system for software vendors who refund the price of software when a purchaser can't install the software on his machine. See Torii's Abstract. Specifically, Torii describes methods for preventing users who properly install software from receiving a refund from the vendor. See col. 1, lines 52-60. To accomplish this, Torii teaches monitoring a user while the user attempts to install software. See col. 7, lines 44-67. Specifically, when a user begins to install software, an "installation state monitoring unit" writes a "start code" in an installation history file. If the installation is completed, a "termination code" is recorded in the installation history file (col. 8, lines 4-10).

When a user requests a refund, the user must send the installation history file to the software vendor. See col. 10, lines 56-64. If the history file has a start code and a termination code, the vendor knows the user successfully installed the software, and the vendor can properly deny the refund. However, if the history file has a start code but lacks a termination code, the vendor knows the user did not install the software, and the vendor would refund the price of the software to the user. See col. 11, lines 25-29.

B. Rejection under 35 U.S.C. §103(a)

1. Claims 1-15

Although independent claims 16 and 17 may be considered broader in some aspects than independent claims 1, 8 and 15, appellants begin with presenting the arguments for patentability of claim 1 because the Examiner's rejection is applied only to the language of claim 1.

As described above claim 1 is directed to a security information mediation apparatus disposed between a first terminal at an information contributor and a second terminal at an information recipient, as illustrated, for example, in FIGS. 1, 4, 8 and 12 of the specification. The security information mediation apparatus includes a first receiving unit, a first registering unit, a first transfer unit, a second receiving unit, a second registering unit and a second transfer unit which work together to perform a process of transferring information about a design error or a bug in a computer program to a developer and if the developer finds the information useful to reward the information provider. Applicants respectfully submit that the features of the security information mediation apparatus operating as claimed in claim 1 are not taught or suggested by Linehan.

In the Office Action mailed on March 27, 2006, the Examiner does not clarify which of the four parties involved in the transaction described in Linehan (the issuing bank, the consumer, the merchant and the acquiring bank) is considered to be the first terminal and which is considered to be the second terminal.

On page 4 lines 3-6 of paragraph 3.2 of the Office Action mailed on March 27, 2006 it is asserted that "Linehan discloses registering information between a merchant and a bank that meets the recitation of a first receiving unit which receives security information from the first terminal a first registering unit which registers the security information in a first database (column 4, lines 9-22)". The indicated paragraph of Linehan states the following:

> The method of the invention includes the step of sending from a consumer's computer a start message over an internet network to a merchant's computer. The merchant's computer then replies to the consumer's computer with a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank. The wallet initiation message includes a payment amount, an order description, a timestamp, and a nonce. This starts a consumer's wallet program in the consumer's computer in response to the wallet initiation message. The consumer's computer then sends over the internet network some consumer identity and authentication information, such as a userid and user password, plus the merchant message, to an issuer gateway operating on behalf of an issuing bank.

The Office Action is in error relative to the teachings of the indicated paragraph. Two communications are described in column 4, lines 9-22 of Linehan: a communication between the consumer and the merchant and a communication between the consumer and the issuer gateway on behalf of the issuer bank. There is no communication between the merchant and any of the banks, the issuer bank and the acquiring bank. Additionally, nowhere in the indicated paragraph is there taught or suggested any operation corresponding to registering information in

a database. Upon reviewing the disclosure of Linehan, Applicants found no other teachings that would cure this deficiency.

Therefore, Applicants respectfully submit that Linehan does not teach or suggest "a first receiving unit which receives security information from the first terminal" and "a first registering unit which registers the security information in a first database" , as recited in claim 1.

Further, on page 4, lines 7-11 of paragraph 3.2 of the Office Action mailed on March 27, 2006, the Examiner asserts that "[Linehan] discloses the bank transferring security information to a gateway service then to the consumer that meets the recitation of the first transfer unit which receives the security information from the first registering unit and transfers the security information registered by the first registering unit to the second terminal for the information recipient to judge the usefulness of the security information (column 4, lines 18-45)". The indicated paragraph states the following:

> The consumer's computer then sends over the internet network some consumer identity and authentication information, such as a userid and user password, plus the merchant message, to an issuer gateway operating on behalf of an issuing bank. The issuer gateway verifies the merchants signature to prove that the consumer is dealing with the actual merchant and validates the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement. The issuer gateway then verifies that the consumer's account is active and has sufficient funds and/or credit to support the payment amount. The issuer gateway then pre-authorizes payment by sending over the internet network an authorization token, an issuer's digital certificate, the wallet initiation message, and a reference value representing the consumer's credit or debit card number. The authorization token includes the payment amount, order description, timestamp, a random nonce plus a merchant identifier and the reference to the consumer's credit or debit card number. The issuer gateway signs the authorization token. This information can be sent either to the consumer or to the merchant to fulfill the order description. If sent to the consumer, the consumer forwards the authorization token to the merchant. The merchant verifies the issuer's signature, issuer's digital certificate, and authorization token contents to validate that the payment is authorized by the issuer.

Applicants do not find in the indicated paragraph the teachings alleged by the Examiner and the features recited in claim 1. None of the banks transfer information in the cited art. One can learn from the indicated portion of Linehan that the issuer gateway sends other information (i.e., "an authorization token, an issuer's digital certificate, the wallet initiation message, and a reference value representing the consumer's credit or debit card number") to the consumer or directly to the merchant based on received information and pre-stored information.

Therefore, Applicants respectfully submit that the issuer gateway or any of the banks in Linehan do not meet the description of "a first transfer unit which receives the security information from the first registering unit and transfers the security information registered by the first registering unit to the second terminal for the information recipient to judge usefulness of the security information" , as recited in claim 1.

Further, on page 4, lines 11-14 of paragraph 3.2 of the Office Action mailed on March 27, 2006, the Examiner asserts that "the issuer gateway receives information for validation that meets the recitation of a second receiving unit which receives at least reply information including the usefulness of the security information from the second terminal (column 4, lines 24-44." The indicated paragraph is reproduced above ("The issuer gateway verifies ... authorized by the issuer.").

The issuer gateway in Linehan indeed performs a number of verification operations and issues new (reply) information, for example, an authorization token based of the security information received from the customer. However, the issuer gateway is not a recipient of the reply information but the source. Therefore, Applicants respectfully submit that the issuer gateway cannot be the same time the second terminal and the second receiving unit. Therefore, the disparate teachings of Linehan cannot be applied in the context of claim 1.

Therefore, Applicants respectfully submit that Linehan does not teach or suggest "a second receiving unit which receives at least reply information including the usefulness of the security information corresponding to the security information from the second terminal."

Further, in the portion between page 4, line 14 of paragraph 3.2 and page 5 line 2 of the Office Action mailed on March 27, 2006, the Examiner asserts that "authorized information is sent to the merchant that meets the recitation of a second registering unit which registers at least the reply information in a second database and a second transfer unit which receives at least the reply information from the second registering unit and transfers the reply information to the first terminal (column 4 lines 34-57)." The indicated paragraph is partially reproduced above (from "The authorization token includes... to authorized by the issuer.") and then states

> Once the merchant has received the authorization token from the issuer gateway, the merchant completes the sales transaction with the consumer. Then later, the merchant sends a message, including the reference value representing the consumer's card number, over the internet to an acquirer gateway operating on behalf of an acquirer bank, to capture the transaction and get paid. The acquiring bank will settle accounts with the issuing bank over a private network by sending a settlement message that includes the reference to the consumer's card number.

The indicated paragraph describes a method of payment for a multi-party transaction (the merchant, the issuer gateway, the acquiring bank and the issuing bank). The paragraph does not teach or suggest any registering of the information in a database, neither transferring the reply information to the first terminal.

Therefore, Applicants respectfully submit that Linehan does not teach or suggest "a second registering unit which registers at least the reply information in a second database" and "a second transfer unit which receives at least the reply information from the second registering unit and transfers the reply information to the first terminal", as recited in claim 1.

On page 5, lines 2-8 of the Office Action mailed on March 27, 2006, the Examiner asserts a long train of statements which mix the language of Linehan and the language of claim 1 making it difficult to determine which features are allegedly taught by Linehan at column 6, lines 20-32. The indicated paragraph refers to FIG. 2B, which illustrates the route of the authorization token in the four-party protocol, and states

> The reference number 252' is created by the issuing bank 212, for example by preparing a table of credit card or debit card numbers 250 and a corresponding table of reference numbers 252. The issuing bank pairs the consumer's card number 250 with a selected reference number 252 and outputs the reference number over path 226' to the issuer gateway 214. The issuer gateway then includes the reference number 252' with the authorization token 254. The authorization token 254 includes the payment amount, order description, timestamp, a random nonce plus a merchant identifier and the reference number 252' to the consumer's credit or debit card number. The issuer gateway 214 signs the authorization token 254 on behalf of the issuing bank 212.

Applicants do not find in the indicated paragraph teachings of a conditional payment based on usefulness of the information via a fee or transferring to the contributor the reply information, as specified in claim 1.

Applicants respectfully submit that Linehan does not teach or suggest "when the information recipient finds that the security information has usefulness, the second receiving unit receives payment information on an information presentation fee to be paid to the information contributor from the second terminal, the second registering unit registers the payment information together with the reply information, and the second transfer unit transfers the payment information together with the reply information to the first terminal."

On page 5, lines 9-19, the Examiner states

> Linehan discloses the invention by the way of example. It is obvious to one skilled in the art that any modification or variation

> such as the order of transmission of data and combining or separating the task into one or many apparatus would be a routine skill in the art and not a patentable invention but rather a design choice. One skilled in the art would have been motivated to combine the functions into one unit to save in resources or/and distribute some functions into many units to separately control the transaction so that if one unit is compromised the entire system is not. To shift location of parts requires routine skill in the art – *In re Japikse* 86 USPQ 70 (CCPA 1950). Using first, second units and databases is a minor modification of the invention disclosed by **Linehan** and one skilled in the art would have been motivated to modify the invention to fit their design need.

Applicants respectfully submit that the differences between Linehan's teachings and claim 1 recitations are neither minor nor inherent as the Examiner seems to argue in the above reproduced paragraph. *In re Japikse*, 181 F.2d 1019, 86 USPQ 70 (CCPA 1950) is a case in which claims to a hydraulic power press read on the prior art except with regard to the position of the starting switch. The claims were held unpatentable because shifting the position of the starting switch would not have modified the operation of the device. However the difference between the system disclosed in Linehan and the apparatus of claim 1 are far more substantial and as argued above one cannot distinguish anything like the features recited in claim 1 in the indicated portions of Linehan. The differences go beyond any of the acceptable deviations listed in MPEP 2144.04.

Further, the courts held that "The mere fact that a worker in the art could rearrange the parts of the reference device to meet the terms of the claims on appeal is not by itself sufficient to support a finding of obviousness. The prior art must provide a motivation or reason for the worker in the art, without the benefit of appellant's specification, to make the necessary changes in the reference device." *Ex parte Chicago Rawhide Mfg. Co.*, 223 USPQ 351 (Bd. Pat. App. & Inter. 1984). The Office Action does not meet the burden of providing a motivation or reason to make the necessary changes in the system disclosed in Linehan.

Claim 1 also recites "security information comprising information regarding a design error or bug in a computer program". The Examiner acknowledges that Linehan does not teach this feature on page 5, lines 21-22. However, the Examiner asserts that Torii "discloses a user storing an installation history file (security information) comprising design error or bug . . in a software . . . (column 10, lines 24-65)".

Information regarding whether software is successfully installed on a machine as disclosed by Torii bears no relation to "a design error or bug in a computer program". As such, a

file containing only a "start code" and a "termination code" does not correspond to this feature of claim 1.

The Examiner also fails to articulate a proper reason to modify Linehan in view of Torii.

> To establish a prima facie case of obviousness . . . there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings.

MPEP § 2143.

The Examiner asserts that one would have modified Linehan to provide "a secure transaction by making sure that the user has proper right of receiving the money, and also a fair transaction by allowing both parties such as the consumer and the software provider to benefit from the transaction." This motivation is improper because, Linehan already provides "a secure transaction". In fact, providing a secure transaction is the exact purpose of the system described by Linehan. As Torii teaches a system that is less secure than the system of Linehan, there is no reason to apply the teachings of Torii to Linehan.

Additionally, Linehan already makes sure that a user has the right to receive money. Again, that is the primary purpose of Linehan, specifically, to ascertain that a merchant has the right to receive money, Linehan explains that a bank "verifies the merchant's signature to prove that the consumer is dealing with the actual merchant and validates the merchant's certification and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement" (col. 6, lines 8-12).

Therefore, Linehan already presents a system that provides "a secure transaction" and "a fair transaction", so that the Examiner fails to articulate a proper reason for modifying Linehan.

For all the above reasons it is submitted that claims 1-15 patentably distinguish over the prior art.

2. Claims 16 and 17

Independent claims 16 and 17 are directed to methods of collecting information over a network. The Examiner, presents no separate reasons for rejecting claims 16 and 17. Applicants respectfully submit that Linehan does not teach the operations recited in claims 16 and 17.

The Linehan disclosure is not related to the claimed "method of collecting information over a network", because information generated and exchanged in a four party transactional system (financial information) is likely privileged or even unconstitutional to share it with a third

party for a fee. Further, Linehan context is not related to "determining that information received from a verified user regarding a security flaw in a product is valuable" and "rewarding the user for submitting the information", because in Linehanen the payment is not sent back to the user (buyer) based on evaluating the information submitted by the customer, but payment is submitted to a third party (the merchant) other than the customer.

Torii does not teach the methods in claim 16 and 17 because in Torii the vendor monitors a user attempt to install a software product via an installation history file. The vendor does not receive information about "a design error or bug in a computer product" as recited in claim 16 or about "a security flaw in a product," as recited in claim 17. Therefore, Torii does not teach "determining that information received from a verified user regarding a security flaw in a product is valuable." Consequently, Torii does not teach or suggest either "rewarding the user for submitting the information."

Therefore claims 16 and 17 patentably distinguish over the prior art.

VIII. Conclusion and Summary

Applicants submit that claims 1-17 patentably distinguish over the prior art. Reversal of the Examiner's rejection is respectfully requested.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Sept. 15, 2006

By: _____
Luminita A. Todor
Registration No. 57,639

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

IX. THE CLAIMS APPENDIX

1. (PREVIOUSLY PRESENTED) A security information mediation apparatus connected between a first terminal at an information contributor and a second terminal at an information recipient, the security information mediation apparatus comprising:

a first receiving unit which receives security information from the first terminal, the security information comprising information regarding a design error or bug in a computer program;

a first registering unit which registers the security information in a first database;

a first transfer unit which receives the security information from the first registering unit and transfers the security information registered by the first registering unit to the second terminal for the information recipient to judge usefulness of the security information;

a second receiving unit which receives at least reply information including the usefulness of the security information corresponding to the security information from the second terminal;

a second registering unit which registers at least the reply information in a second database; and

a second transfer unit which receives at least the reply information from the second registering unit and transfers the reply information to the first terminal, wherein

when the information recipient finds that the security information has usefulness, the second receiving unit receives payment information on an information presentation fee to be paid to the information contributor from the second terminal, the second registering unit registers the payment information together with the reply information, and the second transfer unit transfers the payment information together with the reply information to the first terminal.

2. (PREVIOUSLY PRESENTED) The security information mediation apparatus according to claim 1, wherein said first registering unit refers to the registered security information in the first database, and registers the security information from the first terminal in the first database only if the security information from the first terminal is new, and said first transfer unit transfers the security information from the first terminal to the second terminal only if the security information from the first terminal is new.

3. (PREVIOUSLY PRESENTED) The security information mediation apparatus according to claim 1, further comprising:

a classification information registering unit which registers classification information of the security information desired by the information recipient; and

a classification unit which classifies the security information from the first terminal,

wherein said first transfer unit transfers the security information to the second terminal only if the classification information and classification result of said classification unit coincide.

4. (PREVIOUSLY PRESENTED) The security information mediation apparatus according to claim 1, wherein the second receiving unit receives invalidity information showing invalidity of the security information from the second terminal, and said second transfer unit transfers the invalidity information to the first terminal.

5. (PREVIOUSLY PRESENTED) The security information mediation apparatus according to claim 1, wherein the second receiving unit receives, from the second terminal, correction information as a measure for the security information of which usefulness is shown and said second transfer unit transfers the correction information to the first terminal.

6. (PREVIOUSLY PRESENTED) The security information mediation apparatus according to claim 1, further comprising a disclosing unit which discloses the security information registered by the first registering unit.

7. (PREVIOUSLY PRESENTED) The security information mediation apparatus according to claim 5, further comprising a disclosing unit which discloses the security information registered by the first registering unit and the correction information.

8. (PREVIOUSLY PRESENTED) A security information mediation method, comprising:

receiving security information from a first terminal at an information contributor, the security information comprising information regarding a design error or bug in a computer program;

first registering the security information in a first database;

receiving the security information registered at the first registering and transferring the security information registered at the first registering to a second terminal at an information recipient for judging usefulness of the security information;

receiving at least reply information including the usefulness of the security information corresponding to the security information from the second terminal;

registering at least the reply information in a second database; and

receiving at least the reply information and transferring the reply information to the first terminal, wherein

when the information recipient finds that the security information has usefulness, the receiving of at least the reply information includes receiving payment information on an information presentation fee to be paid to the information contributor from the second terminal, the registering of at least the reply information includes registering the payment information together with the reply information, and the receiving at least the reply information and transferring includes transferring the payment information together with the reply information to the first terminal.

9. (PREVIOUSLY PRESENTED) The security information mediation method according to claim 8, wherein the registering the security information includes referring to the registered security information in the first database, and registering the security information from the first terminal only if the security information from the first terminal is new, and the receiving the security information registered at the first registering step and transferring includes transferring the security information from the first terminal to the second terminal only if the security information from the first terminal is new.

10. (PREVIOUSLY PRESENTED) The security information mediation method according to claim 8, further comprising:

registering classification information of the security information desired by the information recipient; and

classifying the security information from the first terminal,

wherein the receiving the security information registered at the first registering and transferring includes transferring the security information to the second terminal only if the classification information and classification result at the classifying coincide.

11. (PREVIOUSLY PRESENTED) The security information mediation method according to claim 8, wherein the receiving at least reply information includes receiving invalidity information showing invalidity of the security information from the second terminal, and the receiving at least the reply information and transferring transfers the invalidity information to the first terminal.

12. (PREVIOUSLY PRESENTED) The security information mediation method according to claim 8, wherein the receiving at least reply information includes receiving from the second terminal, correction information as a measure for the security information of which usefulness is shown and the receiving at least the reply information and transferring includes transferring the correction information to the first terminal.

13. (PREVIOUSLY PRESENTED) The security information mediation method according to claim 8, further comprising disclosing the security information registered at the first registering step.

14. (PREVIOUSLY PRESENTED) The security information mediation method according to claim 12, further comprising disclosing the security information registered at the first registering step and the correction information.

15. (PREVIOUSLY PRESENTED) A computer readable medium for storing instructions, which when executed by a computer, causes the computer to perform:

first receiving security information from a first terminal at an information contributor, the security information comprising information regarding a design error or bug in a computer program;

registering the security information in a first database;

receiving the security information registered at the first registering and transferring the security information registered at the first registering to a second terminal at an information recipient for judging usefulness of the security information;

receiving at least reply information including the usefulness of the security information corresponding to the security information from the second terminal;

registering at least the reply information in a second database; and

receiving at least the reply information registered at the second registering step and transferring the reply information registered at the second registering step to the first terminal, wherein

when the information recipient finds that the security information has usefulness, the receiving at least reply information includes receiving payment information on an information presentation fee to be paid to the information contributor from the second terminal, the registering at least the reply information includes registering the payment information together with the reply information, and the receiving at least the reply information includes transferring the payment information together with the reply information to the first terminal.

16. (PREVIOUSLY PRESENTED) A method of collecting information over a network, comprising:

determining that information received from a verified user regarding a design error or bug in a computer program is valuable; and

rewarding the user for submitting the information.

17. (PREVIOUSLY PRESENTED) A method of collecting information over a network, comprising:

determining that information received from a verified user regarding a security flaw in a product is valuable; and

rewarding the user for submitting the information.

X. EVIDENCE APPENDIX

Not applicable.

XI. RELATED PROCEEDING APPENDIX

Not applicable.